REMARKS

Entry of this Amendment is respectfully requested in view of the amendments made to the claims and for the remarks made herein.

Claim 1-29 are pending and stand rejected. Claims 1, 2, 8, 13 and 18 have been amended. Claim 30 has been added.

Claims 1-29 stand rejected under 35 USC 103(a) as being unpatentable over Kim (USP no. 5,799,081) in view of Zhang (USP no. 6,550,008) and further in view Applicant's Admitted Prior Art (AAPA).

The instant Office Action states that "Kim does not teach the control information pair includes CCI and a stream identifier, generating a first key in the POD module and a second key in the set-top box ... the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match. ... Zhang teaches the point of deployment module encrypting the information with the first shared key ... and the set-top box decrypting the encrypted information with the second shared key. ... AAPA teaches the reply message including at least one control information pair, each pair having copy control information and a stream identifier.... It would have been obvious ... to combine a control information pair, generating shared keys, and decrypting content when the shared key match, as taught by AAPA, with the system of Kim/Zhang."

Applicant respectfully disagrees with and explicitly traverses the reason for rejecting the claims. However, in the interest of advancing the prosecution of this matter, the independent claims have been amended to more clearly state the invention. More specifically, the claims have been amended to recited the key are generated using "information associated with each respective device." No new matter has been added. Support for the amendment may be found at least on page 11, lines 6-7, which state "where N_{Host} and N_{Module} are two random numbers generated on the host device and deployment module, respectively."

The present invention, as recited in claim 1, for example, recites a system wherein a deployment module generates a first key using information associated with the deployment and the at least one control information pair to encode information and a set-top box generates a second key using information associated with the set-top box and the at least one control information pair to decode the encoded information. The encoded information is correctly decoded when the first and second keys match.

Kim, as the Office Action states, fails to disclose generating first and second keys. Zhang, in one aspect, teaches that the deployment module and the host device may generate shared keys from information received from a third-party source (see, for example, col. 3, lines 56-60, which state, "[i]n addition, using such messages from the head-end the POD module 26 and the host device 24 can generate a session key for encrypting and decrypting messages transmitted between the POD module and the host device."). Zhang further discloses that "[a] random counting mechanism may also be embedded in the authentication process to make it more robust against a 'man-in-the-middle' an a replay attack in which messages transmitted between the POD module and the host device may be monitored by an intruder to break the cipher of the content protection scheme utilized in the receiver. Once entity authentication has been preformed to ensure that the POD module and the host device are both verified units, a shared session key may then be derived to protect messages between the POD module and host device." (see col. 4, lines 9-19).

Zhang, accordingly, teaches that the POD module and the host module generate session keys from information provided by the authentication source. However, Zhang fails to teach or suggest that the keys are generated also using information associated with each respective device, as is recited in the claims.

AAPR is silent with regard to using information associated with the device to generate the session key.

A claimed invention is prima facie obvious when three basic criteria are met. First, there must be some suggestion or motivation, either in the reference themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings therein. Second, there must be a reasonable expectation of success. And, third, the prior art reference or combined references must teach or suggest all the claim limitations.

None of the references cited, individually or in combination, teach or suggest all the elements recited in the above referred-to claims. Even if there were some motivation to combine teachings of the cited references, the combination would not render obvious the invention claimed as the combined device fails to recite all the elements claimed.

For at least this reason, applicant submits that the rejection of the claim 1 has been overcome and the rejection can no longer be sustained. Applicant respectfully requests withdrawal of the rejection and allowance of the claim.

With regard to the remaining independent claims, these claims recite subject matter similar to that recited in claim 1 and were rejected citing the same references used in rejecting claim 1. Thus, applicant's remarks made in response to the rejection of claim 1 are also applicable in response to the rejection of the remaining independent claims.

In view of the amendments made to the claims and for the remarks made with regard to the rejection of claim 1, which are reasserted, as if in full, in response to the rejection of the remaining independent claims, applicant submits that the reason for the rejection of these claims has been overcome and the rejection can no longer be sustained. Applicant respectfully requests withdrawal of the rejection and allowance of the claims.

The other claims in this application are each dependent from the independent claim discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of the patentability of each on its own merits is respectfully requested.

Claim 30 is new. Support for the subject matter recited in claim 30 may be found at least on page 11, lines 6-7, as previously described.

For all the foregoing reasons, it is respectfully submitted that all the present claims are patentable in view of the cited references. Withdrawal of the rejection and issuance of A Notice of Allowance is respectfully requested. A check for $50.00 is enclosed herein to cover one extra claim.

Respectfully submitted,

Dan Piotrowski
Registration No. 42,079

Date: August 7, 2006

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Mail all correspondence to:
Dan Piotrowski, Registration No. 42,079
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9624
Fax: (914) 332-0615

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP AMENDMENT, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on August 7, 2006.

Steve Cha, Reg. No. 44,069
(Name of Registered Rep.)

(Signature and Date)